A TrendLabs Report

2Q Report on Targeted Attack Campaigns

Contents

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Introduction

Highly targeted attacks refer to a category of threats that pertain to intrusions by threat actors or attackers. These attackers aggressively pursue and compromise chosen targets in order to steal sensitive information. These are not conducted through separate attacks; rather, they comprise of a series of attempts over time to get deeper and deeper into a target's network. Each attempt may either succeed or fail, but the overall goal is to penetrate the target's network and acquire information. Malware is typically used as an attack vector, but the real threat involves human operators who adapt, adjust, and improve their methods based on the victim's defenses.

Enterprises should consider targeted attacks a high-priority threat because of the considerable damage they incur. The human and systemic weaknesses that allow an attacker to compromise an organization can be minimized and mitigated with correct practices and solutions. However, these same weaknesses can never be fully resolved.

Trend Micro monitors the targeted attack landscape in order to identify ongoing campaigns and provide additional threat intelligence useful for identifying the existence of these campaigns in an enterprise network. This quarterly report presents the targeted attack campaigns observed and mitigated by Trend Micro based on reported customer cases, as well as our own independently gathered data.

Campaigns Observed in 2Q

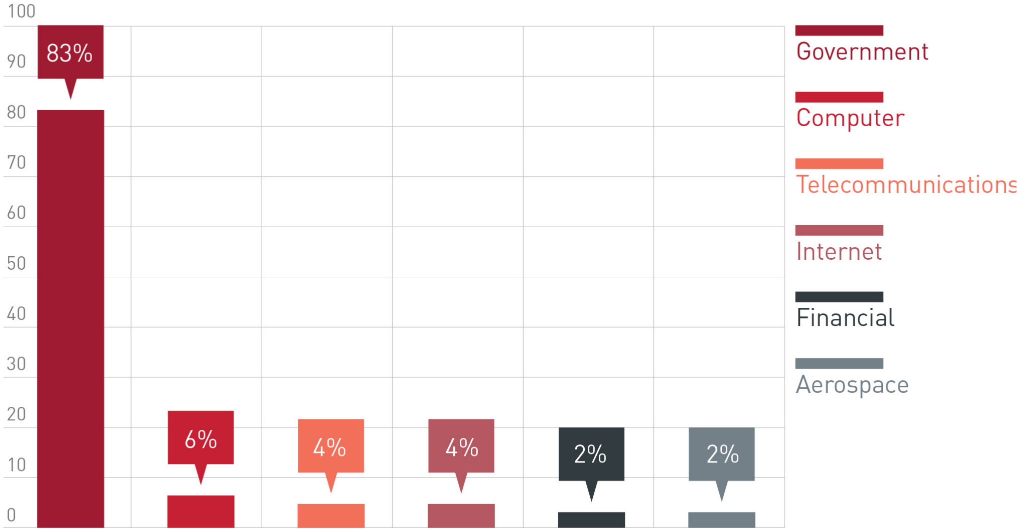
Targeted Attack Campaigns Profiling

We encountered a variety of targeted campaigns in the second quarter of the year. These include the following:

- **IXESHE**. The IXESHE campaign is known for targeting East Asian governments, electronics manufacturers, and telecommunications firms. We released a white paper discussing this campaign.[1] IXESHE has been active since 2012.
- **ELISE**. This recently discovered campaign also targets government agencies in the Asia Pacific region. It is called ELISE after certain strings found in its unpacked code. (We detect the malware used by this campaign as BKDR_ELISE.)
- **ZEGOST.** This family of backdoors (aka HTTP Tunnel) is Chinese in origin and was used in attacks against Asian government organizations.
- **BEEBUS/MUTTER.** This is a targeted campaign believed to be associated with the Comment Crew attacker group because of the use of encrypted/obfuscated HTML comments to hide their C&C transactions.
- **TravNet.** This campaign made use of a malware family identified as NetTraveler based on the strings found in the malware code. The malware is detected as BKDR_TRAVLAR.

Affected Industry Sectors

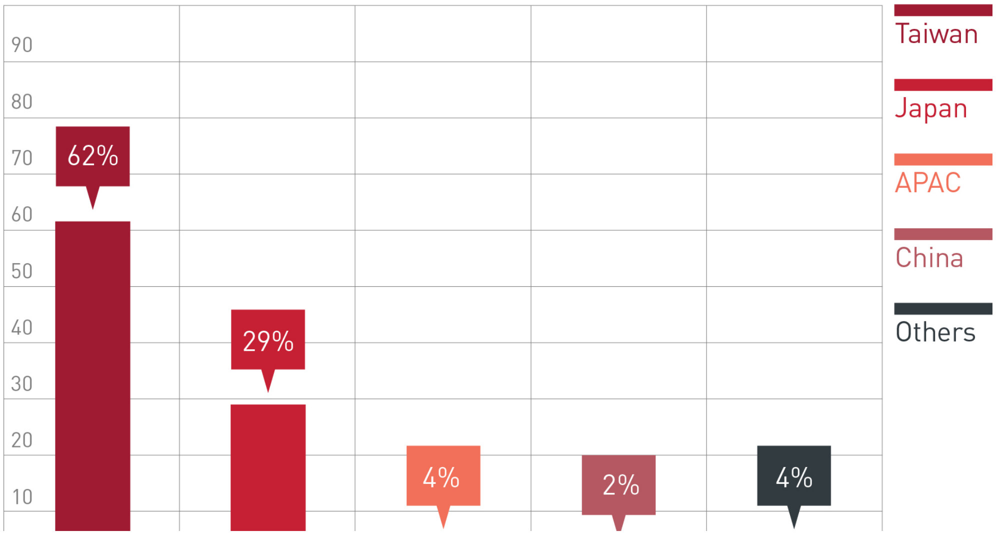
Our data indicates that the majority of targeted attack victims are various government agencies. Targeted firms from the technology sector include telecommunication firms, Internet service providers, and software companies. The financial services sector and the aerospace industry were also targeted this quarter.



Targeted attacks discovered by industry

Affected Regions

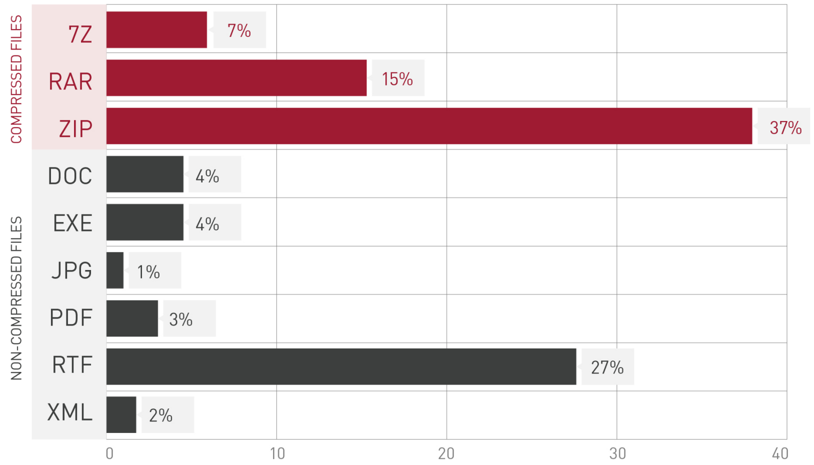
The targeted attacks that we analyzed were heavily concentrated in Asia, particularly Taiwan and Japan.



Targeted attacks discovered by region

Attachments Used In Targeted Attacks

Based on our findings, the most common type of email attachment type used in targeted attacks were file archives of various forms. When uncompressed, these archives typically contain the malicious payload itself, which the user may then run directly. Alternately, they may also contain a .DOC file that contains exploit code. RTF files made up the second most common file type.



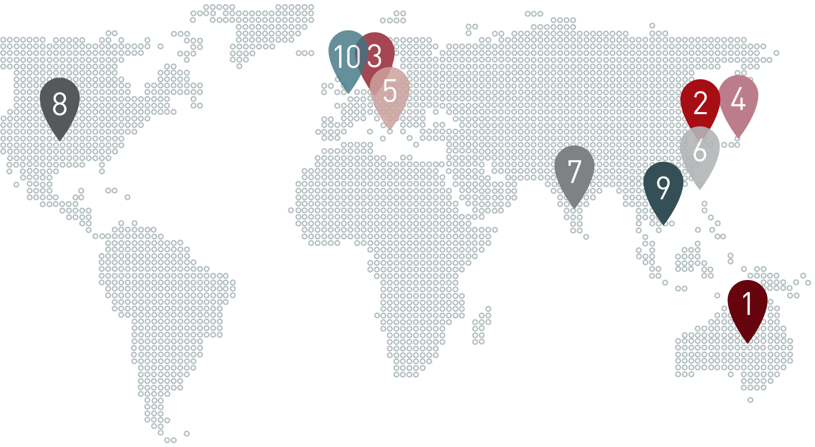
File types used in targeted attacks

Frequently, the .EXE files we see are made to appear as ordinary documents or folders using appropriately chosen icons. In addition, we also saw an increased use of files that make use of right-to-left override (RTLO) in Unicode.

C&C Statistics

We were also able to monitor the activity of various C&C servers related to targeted attacks. By volume of C&C server activity, the following countries ranked as follows:

1	Australia	32%
2	South Korea	15%
3	Germany	9%
4	Japan	7%
5	Italy	6%
6	Taiwan	5%
7	India	4%
8	United States	3%
9	Vietnam	2%
10	Netherlands	2%
	Others	15%



Volume percent of C&C server activity per country

Feature: EvilGrab Campaign Targets Diplomatic Agencies

In this report, we will provide a detailed analysis of the EvilGrab campaign. This campaign was first found targeting certain Asian and European governments. Its name is derived from its behavior of grabbing audio, video, and screenshots from affected machines.

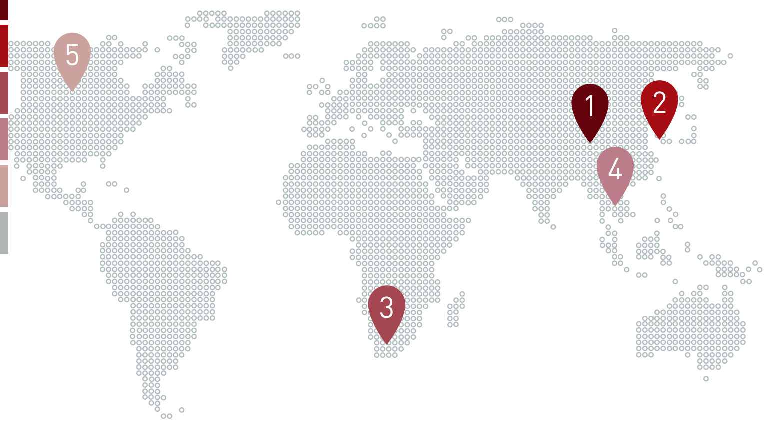
Currently, the malware used by EvilGrab belongs to one of three malware families:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM

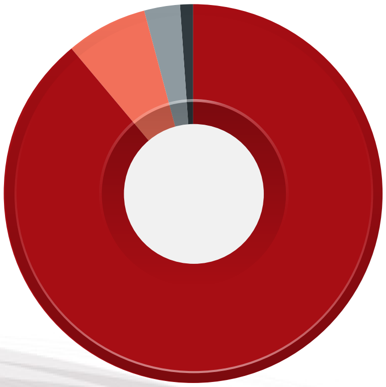
Targets

Our research indicates that EvilGrab activity is most prevalent in China and Japan, although it is also present in other parts of the world. Government organizations were, by far, the most affected by EvilGrab. This geolocation is based on the IP addresses of the victims. Therefore, foreign institutions within China would be identified as coming from China; the same would hold true for all countries. EvilGrab was also found in the United States, Canada, France, Spain, and Australia, among others.

1	China	36%
2	Japan	18%
3	South Africa	3%
4	Thailand	2%
5	Canada	2%
	Others	39%



Map of top affected countries by targeted attacks



1	GOVERNMENT	89%
2	NON-GOVERNMENT ORGANIZATIONS	7%
3	MILITARY	3%
4	ONLINE MEDIA	1%

Sectors affected by targeted attacks

Attack Vectors

Research indicates that EvilGrab is primarily distributed through spear-phishing emails with malicious attachments that exploit various vulnerabilities to run malicious code. Among the attachment types are:

- Microsoft® Excel® spreadsheets (*CVE-2012-0158* and *CVE-2012-2543*)
- PDFs (*CVE-2013-0640*)
- Microsoft® Word® documents (*CVE-2012-0158*)

A .RAR file with a folder named *thumbs.db* was also seen containing malicious code. By using this name, the intention was to disguise itself as the Windows thumbnail cache. A shortcut file (.LNK) was also seen in the .RAR file, which used a folder icon to make users believe it was another folder. In reality, running the .LNK file executes the malware. In addition, the .RAR file contains a *desktop.ini* file in order to change the *thumbs.db* folder icon into the icon of the Windows thumbnail cache.

Exploits, Payloads, and Decoy Documents

The EvilGrab campaign's use of exploits, payloads, and decoy documents is similar to the Taidoor campaign in 2012.[2] The primary difference is that EvilGrab variants have multiple layers of shellcode. In addition, some variants copy the file name and use it as the decoy document file name. Other variants overwrite the exploit document with the contents of the decoy document.

As noted above, some variants also use disguised folders and shortcuts and do not use exploits to run their code.

DLL Preloading Using the Windows Shell and Fax Server

DLL preloading is a vulnerability that has been documented for over three years.[3] The EvilGrab campaign makes use of this vulnerability for its AutoRun routine.

Whenever it is run, the Windows shell (*explorer.exe*) loads a component of the fax server in Windows, *fxsst.dll*. This is normally located in the *System32* folder. Whenever an instance of *explorer.exe* is launched (i.e., at every system startup), the system searches for the said .DLL file and loads it.

EvilGrab drops one of its .DLL components in the Windows folder, where *explorer.exe* is also located. The malicious .DLL (also named *fxsst.dll*) is loaded instead of the legitimate copy. It also serves as the loader of the main backdoor.

While DLL preloading has been used by other malware in the past, it is less common to see it specifically target *explorer.exe*. Other malware families that use this vulnerability typically target executable files outside of Windows; EvilGrab targets a part of Windows itself.

Other Autorun Behaviors

In addition to the above behavior, EvilGrab also creates the following registry entry to enable its automatic execution at every system startup:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
UKey = “%Application Data%\360\Live360.exe”
```

The file *%Application Data%\360\Live360.exe* is a copy of one of the malware components. It also creates a shortcut under the Startup folder in the Start menu:

- *IEChecker.lnk*
    - Target: *"%UserProfile%\IEChecker.exe"* –L
    - Icon: *%Full path of Iexplorer.exe%* (This uses the Internet Explorer icon and disguise itself as part of Internet Explorer.)

The above file is also a copy of one of the malicious components.

Stealth Operation

EvilGrab has three primary components: one .EXE file and two .DLL files. The .EXE file acts as the installer for all of the EvilGrab components. One of the .DLL files serves as a loader for the other .DLL file, which is the main backdoor component. Some variants of EvilGrab delete the .EXE file after installation to cover its tracks more effectively. As noted earlier, the loader file is named *fxsst.dll*. However, examination of its header states that its actual file name is supposed to be *svchost.dll*.

These components are also encrypted and saved in the registry. To add stealth to its backdoor routines, it uses a legitimate process context's memory space to inject the main backdoor.

By default, this backdoor injects itself into the *svchost.exe* or *winlogon.exe* process. It also checks if certain processes related to certain security products are running on the affected system. The specific processes targeted are:

- *avp.exe*
- *klwtblfs.exe*
- *starter.exe*
- *wmifw.exe*

Other variants of this malware also check if other security products are present. It is not clear why EvilGrab specifically targets these products. However, it is possible that the attackers determined that targets for this campaign are likely running these products.

Registry Storage

EvilGrab stores its components in the following registry entries:

```
HKCU\Software\rar and/or HKLM\SOFTWARE\rar
data = {Encrypted copy of the main backdoor DLL}
s = {Encrypted copy of the loader DLL}
e = {Encrypted string which points to the full path of
  the installer EXE}
```

Media Grabbing

To capture video, EvilGrab creates a capture window with the class name of ESET. It uses the Sample Grabber filter (part of the DirectShow technology in Windows) to directly perform grabbing.[4] It also uses Wave APIs to capture audio.[5]

User Credential Theft

EvilGrab steals user credentials related to the following applications and/or protocols:

- HTTP
- HTTPMail
- IMAP
- Internet Explorer (IE)
- Microsoft Outlook

- MSN
- POP3
- Protected Storage
- SMTP
- Windows Messaging

EvilGrab steals these credentials by parsing the following registry keys:

```
• HKCU\Software\Microsoft\Windows NT\CurrentVersion\
  Windows Messaging Subsystem\Profiles
• HKCU\Software\Microsoft\Windows Messaging Subsystem\Profiles
• HKCU\Software\Microsoft\Internet Account Manager\Accounts
• HKCU\Software\Microsoft\Office\Outlook\
  OMI Account Manager\Accounts
```

It queries the above keys for related values that correspond to the applications and protocols listed earlier. The values are then decrypted using the system library *pstorec.dll*.

It also steals login credential from IE autocomplete entries. It does this by first parsing the *index.dat* files in the IE History folder. It then collects autocomplete entries from the following registry key:

```
HKCU\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
```

It then initiates a brute force attack on encrypted credentials using the *CryptUnprotectData* API. However, it will only try to steal passwords from IE's password-protected sites and MSN Explorer Signup if *kav.exe* (related to a security product) is not running in the system.

Tencent QQ Memory Reading

If the active window is Tencent QQ (specifically, QQ2009 through QQ2012), EvilGrab will attempt to steal information by directly reading the process's memory and checking if the class name of the focused window is not named "EDIT."

The contents of the process's memory are then saved onto the system's hard drive as *%UserProfile%\users.bin*. It is then sent back to the backdoor's C&C server. The file on the hard drive is encrypted; specifically, the data is XORed with the key 0x66.

Key Logging

EvilGrab also possesses keylogging capabilities. The logged keystrokes are then sent back to the C&C and saved to *%User Profile%\users.bin*. The file on the hard drive is encrypted; specifically, the data is XORed with the key 0x66.

Command & Control Servers

Each backdoor has one to three C&C servers in its code. Some of C&C servers that we have seen from our accumulated data are as follows:

- 112.121.182.150
- 113.10.246.46
- 113.10.190.55
- 202.130.112.231
- micoosofts.com
- qtds1979.3322.org
- qtds1979.gicp.net
- server1.micoosofts.com
- sxl1979.gicp.net
- webmonder.gicp.net
- webposter.gicp.net
- www.yahooip.net
- www.yahooprotect.com
- www.yahooprotect.net
- yacooll.com
- yahooip.net
- yahooprotect.com

Backdoor Activity

To start its connection to its C&C server, the backdoor component will first send 5-bytes (\x01\x00\x00\x00\x33). The C&C will reply if it accepts the connection. The backdoor then replies with a beacon message, the contents of which are as follows:

Description	Sample value (referring to sample packet illustrated below)
Size of internal buffer	<%d> =xFFC (4092)
Hardcoded 0xA0	<%c> = xA0
Backdoor identifier 1	<%s> = "RB0318"
Host IP	<%s> = "111.222.123.132"
Host port	<%d> = 432 (1074.)
OS version	<%s> = "OSVERSION"
Hostname	<%s> = "HOSTNAME"
User name	<%s> = "USERNAME"
Camera device detected	<%s> = "No"
Date time	<%s> = "0Ìì0Ð¡Ê±0•Ö0Ãë"
Presence of removable drive	<%s> = "No"
Backdoor identifier 2	<%s> = "V2010-v24"
Process ID of the process where the backdoor is injected	<%d> = 21C (540.)
Hardcoded 0x00	<%d> = 0

Either backdoor identifier 1 or backdoor identifier 2 acts as the campaign code or marker for EvilGrab campaigns, which is recognizable by the C&C server and/or attacker. Some of the identifiers we saw in backdoor identifier 1 are:

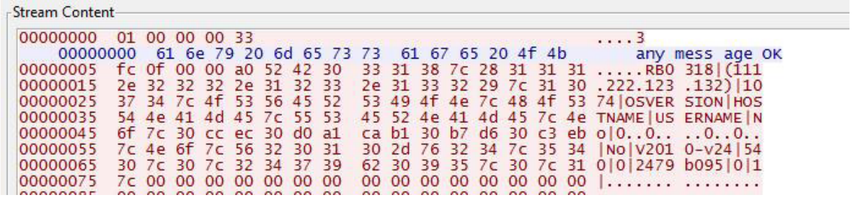
- 006
- 007
- 0401
- 072002
- 3k-Ja-0606
- 3k-jp01
- 4k-lyt25
- 88j
- e-0924
- LJ0626
- RB0318

Some of the identifiers seen in our accumulated data in backdoor identifier 2 are as follows:

- V2010-v16
- V2010-v24

We noted a correlation between the MZ/PE headers of variants and the strings in backdoor identifier 2. Variants with a V2010-v24 identifier have a proper MZ/PE header; variants with a V2010-v16 header have portions of their header overwritten with JPEG strings. These variants require a loader component to load them into memory in order to be executed.

Below is a sample packet sent at the beginning of the connection:



Stream Content

```
00000000  01 00 00 00 33                                       ....3
    00000000  61 6e 79 20 6d 65 73 73  61 67 65 20 4f 4b           any mess age OK
00000005  fc 0f 00 00 a0 52 42 30  33 31 38 7c 28 31 31 31 .....RB0 318|(111
00000015  2e 32 32 32 2e 31 32 33  2e 31 33 32 29 7c 31 30 .222.123 .132)|10
00000025  37 34 7c 4f 53 56 45 52  53 49 4f 4e 7c 48 4f 53 74|OSVER SION|HOS
00000035  54 4e 41 4d 45 7c 55 53  45 52 4e 41 4d 45 7c 4e TNAME|US ERNAME|N
00000045  6f 7c 30 cc ec 30 d0 a1  ca b1 30 b7 d6 30 c3 eb o|0..0.. ..0..0..
00000055  7c 4e 6f 7c 56 32 30 31  30 2d 76 32 34 7c 35 34 |No|V201 0-v24|54
00000065  30 7c 30 7c 32 34 37 39  62 30 39 35 7c 30 7c 31 0|0|2479 b095|0|1
00000075  7c 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |....... ........
```

Code snapshot

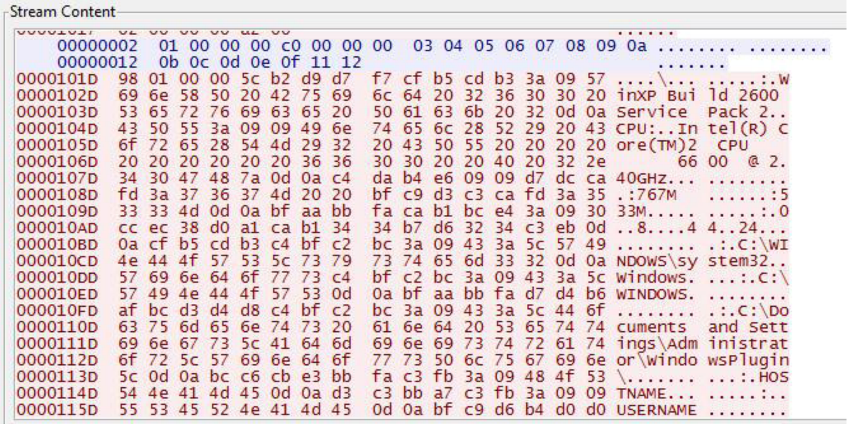
EvilGrab variants possess a wide variety of possible backdoor commands. The table below lists its possible commands:

Command code	Description
x82	Enumerate drives and their drive types
x83	File listing with file's last modification date, file attribute and file size
x85	Execute downloaded file
x86	Set file pointer of specific file
x87	Close file handles
x88	Load .DLL
x89	Create directory
x8A	Delete file
x8B	Delete directory tree
x8C	Get file time stamps of a specific file
x8E	Either runs an executable, loads a DLL or open a file
x8F	Move/Rename a file
x90	Steal login credentials

Command code	Description
x92	Create remote shell
x93	Write to file
x94	Close thread that created remote shell
x99	Send message to a certain window
x9A - x9B	Related to change a specific window's show state
x9C	Change window text of certain window
x9D, x9F	Synthesize key strokes (i.e. right menu, shift)
xB0	Triggers sending of accumulated stolen information
xB1	Modify registry entry value
xB2	Delete a value from registry
xB4	Modify registry
xB5	Create registry entry
xB7	Delete registry key
xB9	Get service listing info (service name, service type, service status, service setting)
xBA	Change service status
xBB	Change optional parameters of certain services
xBC	Create service

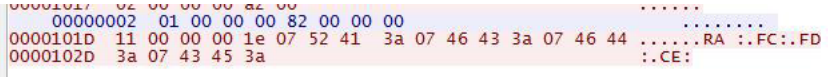
Command code	Description
xBD	Get TCP & UDP network connections
xBE	Get process listing
xBF	Terminate process
xC0	Get CPU info, Windows and System32 folder, hostname, user name, clipboard contents
xC1	Delete its files and registries from the system (uninstall itself)
xE2- xE3	Related to stealing desktop screenshots
xE5	Get desktop screenshot
xE6	Get file listing
xE9	Connect to other network
xEB	Set mouse event
xEC	Start capture window for media grabbing
xEE	Media capture related
xF0	Start audio recording
xF2	Search for certain files and steal file content

This captured packet shows sample backdoor commands and replies:



```
00001017  02 00 00 00 a2 00                                ......
    00000002  01 00 00 00 c0 00 00 00  03 04 05 06 07 08 09 0a ........ ........
    00000012  0b 0c 0d 0e 0f 11 12                             .......
0000101D  98 01 00 00 5c b2 d9 d7  f7 cf b5 cd b3 3a 09 57 ....\... .....:.W
0000102D  69 6e 58 50 20 42 75 69  6c 64 20 32 36 30 30 20 inXP Bui ld 2600 
0000103D  53 65 72 76 69 63 65 20  50 61 63 6b 20 32 0d 0a Service  Pack 2..
0000104D  43 50 55 3a 09 09 49 6e  74 65 6c 28 52 29 20 43 CPU:..In tel(R) C
0000105D  6f 72 65 28 54 4d 29 32  20 43 50 55 20 20 20 20 ore(TM)2  CPU    
0000106D  20 20 20 20 20 20 36 36  30 30 20 20 40 20 32 2e       66 00  @ 2.
0000107D  34 30 47 48 7a 0d 0a c4  da b4 e6 09 09 d7 dc ca 40GHz... ........
0000108D  fd 3a 37 36 37 4d 20 20  bf c9 d3 c3 ca fd 3a 35 .:767M   ......:5
0000109D  33 33 4d 0d 0a bf aa bb  fa ca b1 bc e4 3a 09 30 33M..... .....:.0
000010AD  cc ec 38 d0 a1 ca b1 34  34 b7 d6 32 34 c3 eb 0d ..8....4 4..24...
000010BD  0a cf b5 cd b3 c4 bf c2  bc 3a 09 43 3a 5c 57 49 ........ .:.C:\WI
000010CD  4e 44 4f 57 53 5c 73 79  73 74 65 6d 33 32 0d 0a NDOWS\sy stem32..
000010DD  57 69 6e 64 6f 77 73 c4  bf c2 bc 3a 09 43 3a 5c Windows. ...:.C:\
000010ED  57 49 4e 44 4f 57 53 0d  0a bf aa bb fa d7 d4 b6 WINDOWS. ........
000010FD  af bc d3 d4 d8 c4 bf c2  bc 3a 09 43 3a 5c 44 6f ........ .:.C:\Do
0000110D  63 75 6d 65 6e 74 73 20  61 6e 64 20 53 65 74 74 cuments  and Sett
0000111D  69 6e 67 73 5c 41 64 6d  69 6e 69 73 74 72 61 74 ings\Adm inistrat
0000112D  6f 72 5c 57 69 6e 64 6f  77 73 50 6c 75 67 69 6e or\Windo wsPlugin
0000113D  5c 0d 0a bc c6 cb e3 bb  fa c3 fb 3a 09 48 4f 53 \....... ...:.HOS
0000114D  54 4e 41 4d 45 0d 0a d3  c3 bb a7 c3 fb 3a 09 09 TNAME... .....:..
0000115D  55 53 45 52 4e 41 4d 45  0d 0a bf c9 d6 b4 d0 d0 USERNAME ........
```

Backdoor command xC0: Get CPU info, Windows and System32 folder, hostname, user name and clipboard content



```
00001017  02 00 00 00 a2 00                                ......
    00000002  01 00 00 00 82 00 00 00                      ........
0000101D  11 00 00 00 1e 07 52 41  3a 07 46 43 3a 07 46 44 ......RA :.FC:.FD
0000102D  3a 07 43 45 3a                                   :.CE:
```

Backdoor command x82: Get drive listings and types

These capabilities can be used for both lateral movement within a compromised organization and to steal information. EvilGrab steals internal user names and passwords as well as logs keystrokes. Credentials stolen this way can be used to move within the confines of the organization's network.

EvilGrab possesses a wide variety of information theft capabilities. It can grab audio and video files directly from devices attached on the system (i.e. microphone and camera). In addition, EvilGrab can upload files from the affected system to remote servers. EvilGrab possesses a full range of capabilities that is expected in malware used in targeted attacks against organizations.

Trend Micro Recommendations

Targeted attacks pose a challenge to traditional signature-based security solutions. To deal with these type of threats, employ solutions that include network monitoring to detect and analyze incoming threats, as well as any outgoing communication with attacking parties.

Products like Trend Micro™ Deep Discovery™ are capable of mitigating the risks from these threats. One component of Deep Discovery, the Deep Discovery Inspector, provides network threat detection, custom sandboxing, and real-time analysis and reporting.

The second component, Deep Discovery Advisor, provides sandbox analysis of known and unknown threats that augments the capabilities of existing products like endpoint solution and email/web gateways. It also provides visibility to network-wide security events.

The capabilities provided by solutions like Deep Discovery are necessary to provide a unified, comprehensive view of the threats an organization faces. This information can then be used by an organization to create appropriate and proportional responses to properly protect an organization's network.

References

1 Sancho, David; Dela Torre, Jessa; Bakuei, Matsukawa; Villeneuve, Nart; and McArdle, Robert. (2013). *Trend Micro Incorporated Research Paper*. "IXESHE: An APT Campaign." Last accesed August 30, 2013. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

2 Trend Micro Incorporated. (2013). *Trend Micro Incorporated Research Paper* "The Taidoor Campaign: An In-Depth Analysis." Last accessed August 30, 2013. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf

3 Security TechCenter. (November 13, 2012). *Microsoft Security Advisory*. "Microsoft Security Advisory (2269637): Insecure Library Loading Could Allow Remote Code Execution" Last accessed August 30, 2013. http://technet.microsoft.com/en-us/security/advisory/2269637

4 Microsoft. (2013). *Windows Dev Center - Desktop*. "Using the Sample Grabber." Last accessed August 30, 2013. http://msdn.microsoft.com/en-us/library/windows/desktop/dd407288(v=vs.85).aspx

5 Microsoft. (2013). *Developer Network*. "Recording and Playing Sound with the Waveform Audio Interface." Last accessed August 30, 2013. http://msdn.microsoft.com/en-us/library/aa446573.aspx#waveinout_topic_006

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003